UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

PAUL MALICK and MARGARET MALICK, Individually And On Behalf of All Others Similarly Situated,	:	Case No. _____
Plaintiffs,	:	
–v.	:	
EXCELLUS HEALTH PLAN, INC., and LIFETIME HEALTHCARE, INC.,	:	CLASS ACTION COMPLAINT JURY TRIAL DEMANDED
Defendants.	:	

Plaintiffs Paul Malick and Margaret Malick ("Plaintiffs") individually, and on behalf of all others similarly situated, by and through counsel, bring this action against Defendants Excellus Health Plan Inc., better known as Excellus Blue Cross Blue Shield, and Lifetime Healthcare Inc., f/k/a Excellus, Inc. (collectively, "Defendants"), and state as follows:

NATURE OF THE CASE

1. This is a consumer class action lawsuit brought against Defendants for their failure to safeguard and secure the medical records, and other personally identifiable information, including names, dates of birth, social security numbers, billing information, and other types of information ("PII") and highly confidential and personal health-related information ("PHI") of Plaintiffs and Class Members. PHI and PII collectively shall be referred to as "Personal Information." On or about August 5, 2015, Defendants acknowledged that their system had been breached and the Personal Information of over ten million policyholders had been compromised (the "Breach"). This Breach is the result of Defendants' failure to

implement cybersecurity measures commensurate with the duties it undertook in storing vast quantities of PII.

2. On information and belief, Plaintiffs' PHI and PII were disclosed in the data breach.

3. Defendants failed to keep safe their customers' sensitive private, financial, medical and personal information.

4. Defendants breached their duty to protect and safeguard their customers' Personal Information and to take reasonable steps to mitigate the damage caused. Defendants' failure to protect their customers' Personal Information has caused damage to Plaintiffs and the approximately ten million Class Members they seek to represent.

PARTIES

5. Plaintiffs Paul Malick and Margaret Malick are residents and citizens of Rochester, Monroe County, New York.

6. Plaintiffs Paul Malick and Margaret Malick had medical insurance coverage through Excellus BlueCross BlueShield, offered through Mr. Malick's employer. Plaintiffs cancelled their coverage with Excellus BlueCross BlueShield in 1990.

7. On or about September 20, 2015, both Plaintiff Paul Malick and Plaintiff Margaret Malick received a notice from Excellus BlueCross BlueShield stating that their Personal Information had been compromised in a data breach. Both notices were dated September 17, 2015.

8. In providing this information to Defendants and paying their insurance premiums in exchange for medical insurance coverage, Plaintiffs did not consent to relinquish control over their Personal Information or allow their Personal Information to be disclosed and publicized.

They are greatly troubled by the loss of control over their PII and PHI and/or publication of their Personal Information, and maintain that they paid part of their insurance premium to ensure reasonable security of their Personal Information. Plaintiffs also feel stress over their loss of control over their Personal Information and/or publication of their Personal Information, which they fear will subject them to lifelong exposure to identity theft, medical data misuse and other repercussions.

9. Due to the extremely problematic nature of the loss of control and/or publication of Plaintiffs' Personal Information, their resulting stress, and Defendants' lack of timely notice and inadequate response to the Breach, Plaintiffs have expended time attempting to safeguard themselves from identity theft and other harms caused by the release of their PII and PHI as a result of the Breach. Going forward, Plaintiffs anticipate spending considerable time in an effort to contain the impact of Defendants' Breach as it relates to their Personal Information that, on information and belief, is now in the public domain.

10. Plaintiffs have not received notice from any other company of a potential breach with regard to their Personal Information.

11. Defendant Excellus Health Plan, Inc. ("Excellus") is a New York corporation with their principal place of business located in Rochester, New York.

12. Defendant Lifetime Healthcare Inc., f/k/a Excellus, Inc. ("Lifetime") is a New York not-for-profit corporation with their principal place of business located in Rochester, New York.

13. Defendant Excellus operates as a wholly-owned subsidiary of Lifetime and is a licensee of the Blue Cross and Blue Shield Association. Defendant Excellus is the primary health care provider in upstate New York, with regional headquarters in Rochester, Syracuse,

Elmira, and Utica, and field offices in Watertown, Binghamton, Oneonta, and Plattsburgh. Defendant Excellus is the parent of two health maintenance organizations ("HMOs") in the New York State Health Insurance Program: Blue Choice and HMO Blue. In addition, Defendant Excellus maintains relationships with several affiliates of Lifetime, including Lifetime Benefit Solutions, Lifetime Care, Lifetime Health Medical Group, MedAmerica Companies, and Univera Healthcare.

14. Defendant Lifetime has confirmed that all of their affiliates were impacted by the Data Breach, including Excellus BlueCross BlueShield, Lifetime Benefit Solutions, Inc., Lifetime Care, Lifetime Health Medical Group, MedAmerica Insurance Company, and Univera Healthcare.

JURISDICTION AND VENUE

15. This Court has original jurisdiction pursuant to 28 U.S.C. §1332(a)(1) and (d)(2). In the aggregate, Plaintiffs' claims and the claims of the other Members of the Class exceed $5,000,000 exclusive of interest and costs, there are 100 or more class Members, and this a class action in which some Members of the Class are citizens of states other than Defendants.

16. This Court also has personal jurisdiction over Defendants because Defendants are organized and incorporated under New York law, are licensed and registered to do business in New York, regularly conduct business in New York, and have their principal place of business in Rochester, New York.

17. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendants are headquartered in this District and regularly conduct business in this District, Plaintiffs reside in this District, a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, and Defendants have caused harm to Class Members

residing in this District.

FACTUAL BACKGROUND

18. Defendant Excellus is one of the largest healthcare providers in New York.

19. Defendants understand that their customers place a premium on privacy. Defendant provide each of their customers with a notice of privacy practices.[1] Defendants' notice of privacy practices assures their customers that Defendants are "committed to safeguarding" their customers' "protected health information," and states that they are "required by applicable federal and state laws to maintain the privacy" of personal customer information. Defendants' notice further warrants that they will not provide any nonpublic information without individual consent. Nonpublic information is defined as, *inter alia*, "names, Member identification number, social security number, addresses, type of health care benefits, payment amounts, etc."

20. Defendants also dedicate a section of their website to explain their privacy and data collection policies.[2] The Privacy Policy on the website adds assurances that Defendants are "committed to protecting any personal information" that individuals provide. Defendants further stress that the collection of Personal Information is required in order to obtain healthcare services. Defendants note, however, that customers need not worry: "Personally Identifiable Information you provide to Excellus BlueCross BlueShield via this website will only be used for the express purpose of your disclosure to us, unless otherwise described herein."

21. The statements on Defendants' website and in their notice of privacy practices

[1] Excellus Privacy Policy available at https://www.excellusbcbs.com/wps/portal/xl/mbr/mgr/manageprivacy/ (last visited October 22, 2015).

[2] https://www.excellusbcbs.com/wps/portal/xl/!ut/p/b1/lYtLDoIwFADP4gn6KK8tLltLwQZBCxrpxnRBCAmfjfH8SlwbdXaTzBBP2ghQMIwREnIlfg6PoQ_3YZnDuLrnt-bssBA5heqiGOwpc-lJpzFU_BW0awDSCVGYGjFrIGLlDuHNb39mea3tVnGFB-BW0yP89cMH5Ne_zJepI5MfjUnk5gmKzEns/dl4/d5/L2dJQSEvUUt3QS80SmtFL1o2X1QwQVI3N0xGUzQ0R1QwMTVNQkEwMDAwMDAw/ (last visited October 22, 2015).

make clear that Defendants are aware of the importance their customers place on privacy, as well as their duty to safeguard and protect Personal Information that their customers supply, and to provide prompt notice to customers if any PHI and/or PII is compromised.

THE BREACH

22. In December 2013, hackers gained access to the data systems of Excellus. For the next 20 months, these intruders operated undetected in the data systems of Excellus. Defendants did not discover that hackers were in their system until August 5, 2015.

23. Based on the message from the President and CEO Christopher Booth on Defendants' data breach information website, www.excellusfacts.com (the "Breach Website"), hackers gained access to highly sensitive and confidential personal, health, and financial information, including names, dates of birth, Social Security numbers, mailing addresses, telephone numbers, Member identification, financial payment information, and medical insurance claims information. Some of this financial payment information included credit card numbers.

24. Defendants have acknowledged that because hackers had access to their network and went undetected for so long, the hackers would have been able to circumvent any data encryption, likely accessing decryption keys available to administrators on the system.

25. Defendants did not publicly disclosed the Breach until on or about September 9, 2015. Defendants have stated that between 10 and 10.5 million individuals were affected. The affected individuals include not only past and current Excellus policyholders, but also those insured through Defendants' affiliates. Members of the Blue Cross Blue Shield network who received treatment in the upstate New York service area of Defendants are also likely affected.

26. On the Breach Website, Mr. Booth further stated that safeguarding the privacy of

their customers' Personal Information was a "top priority" and that Defendant "make[s] every effort" to protect the PII and PHI of their insureds. Mr. Booth informed Breach victims that Defendant would offer two years of credit monitoring through third-party provider Kroll, Inc., and that they remained "committed" to ensuring that victims "get the tools and assistance" needed for protection.

27. Defendants' Breach Website indicates that all affected individuals will receive a Breach notification letter on or before November 9, 2015. Defendant has not explained why it waited approximately one month before disclosing the Breach, or why it may take almost two additional months for all affected individuals to receive the Breach notification letter.

THE CONSEQUENCES OF DEFENDANTS' CONDUCT

28. The Personal Information compromised in the Breach is particularly valuable to thieves. The compromised data leaves Defendants' customers especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

29. The information Defendants lost, including Plaintiffs' PHI and PII is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC") Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration dates, and other information, without permission, to commit fraud or other crimes. The FTC estimates that as many as 9 million Americans have their identities stolen each year. [3]

30. Identity thieves can use identifying data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on

[3] FTC, *About Identity Theft*, available at <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html> (last visited October 22, 2015).

existing accounts, or clone ATM, debit, or credit cards. [4]

31. Recently, Intel Security Group's McAfee Labs released a report on the prices of stolen data on the cyber marketplace. With the dollar value of personal data following the supply/demand business model, this report describes stolen identifying data as the "oil of the digital economy." The report cites the proliferation of businesses established to sell stolen identifying information and the increasing prices for such data as the reason for the growing number of cyber attacks. [5]

32. Identity thieves can use PHI and PII, such as that which Defendants failed to keep secure, to perpetrate a variety of crimes that do not cause financial loss, but nonetheless harm the victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

33. In addition, identity thieves may get medical services using the Plaintiffs' PHI and PII or commit any number of other frauds, such as obtaining a job, procuring housing or even giving false information to police during an arrest.

34. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2008: [6]

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or

[4] *Id.*
[5] *See*, McAfee Labs, *The Hidden Data Economy: The Marketplace for Stolen Digital Information*, available at http://www.mcafee.com/us/resources/reports/rp-hidden-data-economy.pdf (last visited November 3, 2015).
[6] *The President's Identity Theft Task Force Report* at p.21 (Oct. 21, 2008), available at http://www.idtheft.gov/reports/StrategicPlan.pdf (last visited October 22, 2015).

criminal record fraud, face other types of harm and frustration.

> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

35. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches: [7]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

36. "In addition to the financial harm associated with other types of identity theft, victims of medical identity theft may have their health endangered by inaccurate entries in their medical records. This inaccurate information can potentially cause victims to receive improper medical care, have their insurance depleted, become ineligible for health or life insurance, or become disqualified from some jobs. Victims may not even be aware that a theft has occurred because medical identity theft can be difficult to discover, as few consumers regularly review their medical records, and victims may not realize that they have been victimized until they receive collection notices, or they attempt to seek medical care themselves, only to discover that they have reached their coverage limits." [8]

37. "With the advent of the prescription drug benefit of Medicare Part D, the

[7] GAO, *Report to Congressional Requesters*, at p.33 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited October 22, 2015).

[8] *Id.* at 30.

Department of Health and Human Services' Office of the Inspector General (HHS OIG) has noted a growing incidence of health care frauds involving identity theft." Identity thieves can use such information "fraudulently to enroll unwilling beneficiaries in alternate Part D plans in order to increase . . . sales commissions" or commit other types of fraud. "The types of fraud that can be perpetrated by an identity thief are limited only by the ingenuity and resources of the criminal." [9]

38. Medical records and accounts are becoming targets for cyber thieves because these records contain all of the information – name, date of birth, social security number, Medicare number, etc. – that is needed to conduct fraudulent business in the victim's name. [10]

39. Defendants' proposed customer solutions do nothing to address the problem of medical identity theft, and Defendants have done nothing to advise their customers how to obtain and inspect their medical records for fraud to comport with best practices identified by security experts. Further, stolen medical and clinical information may be improperly disclosed for use to discriminate in the provision of healthcare to insureds and prospective insureds. Individuals risk denial of coverage, improper "redlining," and denial or difficulty obtaining disability or employment benefits because information was improperly disclosed to a provider.

40. A recent PricewaterhouseCoopers report stated that an identity theft kit containing health insurance credentials can be worth up to $1,000 on the black market, while stolen credit cards may go for $1 each. [11]

41. The unauthorized disclosure of Social Security Numbers can be particularly damaging, because Social Security Numbers cannot easily be replaced. In order to obtain a new

[9] *Id.* at 31.
[10] http://krebsonsecurity.com/2015/04/a-day-in-the-life-of-a-stolen-healthcare-record/ (accessed November 3, 2015).
[11] http://www.pwc.com/sg/en/publications/assets/cyber-risks-in-interconnected-world-201410.pdf, pg.22 (last visited October 28, 2015).

number, a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration ("SSA") warns:[12]

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other personal information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you will not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.

42. Plaintiffs and the proposed Class now face years of constant monitoring of their financial and medical records, potential identity theft, and loss of rights.

43. When Defendants disclosed the Breach, they announced that they would offer free credit monitoring services for two years. While this gesture is not worthless, credit monitoring services offer little to thwart fraud from occurring, but rather merely informing individuals of fraud after the fact. Defendants' chosen service, provided by Kroll, is deficient in that it only monitors victim's credit at one of the three major credit bureaus. Further, Defendants are not offering credit monitoring for any minor victims nor providing any information on how to protect minor victims from identity theft.

44. The history of cybersecurity breaches in the industry, and the warnings that are

[12] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Aug. 2009), available at http://www.ssa.gov/pubs/10064.html (last visited October 22, 2015).

now all but ubiquitous, placed Defendants on notice of the duty to safeguard their customers' Personal Information. Defendants nonetheless ignored the warning signs and permitted their customers' PII and PHI to be compromised. Defendants should have and could have done more to fulfill their duty to safeguard their customers' sensitive personal, medical, and financial information.

CLASS ALLEGATIONS

45. Plaintiffs bring this action on their own behalf, and on behalf of all other persons nationwide similarly situated and, alternatively, a New York Class (collectively, "the Class").

46. The Nationwide Class that Plaintiffs seek to represent is initially defined as:

> All persons in the United States who were current or prior insureds of Defendants and/or their affiliates as of August 5, 2015, and all persons in the United States who were not insured by Defendant and/or their affiliates as of August 5, 2015 but who are or were Blue Cross Blue Shield customers who received medical treatment in Defendants' upstate New York service area on or before August 5, 2015.

47. The New York Class is initially defined as:

> All persons who reside in New York who were current or prior insureds of Defendants and/or their affiliates as of August 5, 2015, and all persons who reside in New York who were not insured by Defendant and/or their affiliates as of August 5, 2015 but who are or were Blue Cross Blue Shield customers who received medical treatment in Defendants' upstate New York service area on or before August 5, 2015.

48. Excluded from the Class are Defendants; officers, directors, and employees of Defendants; any entity in which Defendants have a controlling interest; the affiliates, legal representatives, attorneys, heirs, and assigns of the Defendants, and all judges to whom the case is assigned, and the Members of their respective staff.

49. Plaintiffs reserve the right to modify or amend the Class definitions before the

Court determines whether class certification is appropriate

50. *Numerosity:* The Members of the Class are so numerous that the joinder of all Members is impractical. While the exact number of Class Members is unknown to Plaintiffs at this time, Defendants have acknowledged that as many as 10 million records may have been compromised in the Breach. The identity of proposed Class Members is ascertainable and can only be determined based upon Defendants' records.

51. *Typicality:* Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PHI and PII, like that of every other Class Member, was misused and/or disclosed by Defendants. Plaintiffs' claims are typical of the claims of the Members of the class because, *inter alia*, all Class Members were damaged by Defendants' misconduct that permitted the Breach to occur. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all Members of the Class.

52. *Existence and Predominance of Common Questions of Fact and Law*: This action satisfies the requirements of Federal Rule of Civil Procedure 23(b)(3) because it involves questions of law and fact common to the Member of the Class that predominate over any questions affecting only individual Members, including, but not limited to:

a. Whether Defendants owed a duty to Plaintiffs and Members of the Class to take reasonable measures to safeguard their Personal Information;

b. Whether Defendants unlawfully used, maintained, lost or disclosed Class Members' PHI and PII;

c. Whether Defendants unreasonably delayed in notifying affected customers of the data breach;

d. Whether Defendants failed to implement and maintain reasonable security

procedures and practices appropriate to the nature and scope of the information compromised in the data breach;

e. Whether Defendants' conduct was negligent;

f. Whether Plaintiffs and the Class are entitled to damages and/or injunctive relief; and,

g. The amount and nature of such relief to be awarded to Plaintiffs and the Class.

53. *Adequacy:* Plaintiffs will fairly and accurately represent the interests of the Class because Plaintiffs fit within the Class definition and Plaintiffs' interests do not conflict with the interests of the Members of the proposed Class Plaintiffs seek to represent. Plaintiffs are committed to the vigorous prosecution of this action. Plaintiffs are represented by experienced Class Counsel. Plaintiffs' Counsel has litigated numerous class actions and intends to prosecute this action vigorously for the benefit of all Class Members. Plaintiffs and their Counsel can fairly and adequately protect the interests of all of the Members of the proposed Class.

54. *Superiority:* The class action is the best available method for the efficient adjudication of this litigation because individual litigation of Class Members' claims would be impracticable and individual litigation would be unduly burdensome to the courts. Plaintiffs and Members of the proposed Class have suffered irreparable harm as a result of Defendant's conduct. Because of the size of each Class Member's claims, no Class Members could afford to seek legal redress for the wrongs identified in this Complaint. Without the class action vehicle, the proposed Class would have no reasonable remedy and would continue to suffer losses, and Defendant would be permitted to retain the proceeds of

its violations of law. Further, individual litigation has the potential to result in inconsistent or contradictory judgments. A class action in this case presents fewer management problems and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

45. Even if the proposed Class Members themselves could afford such individual litigation, the court system could not. Given the complex legal and factual issues involved, individualized litigation would significantly increase the delay and expense to all parties and to the Court. Individualized litigation would also create the potential for inconsistent or contradictory rulings. By contrast, a class action presents far fewer management difficulties, allows claims to be heard which might otherwise go unheard because of the relative expense of bringing individual lawsuits, and provides the benefits of adjudication, economies of scale and comprehensive supervision by a single court.

COUNT I – NEGLIGENCE

55. Plaintiffs repeat, re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

56. Defendants required Plaintiffs and Class Members to submit PII and PHI in order to acquire coverage under a health insurance policy and/or receive medical treatment. Defendants collected and stored this Personal Information.

57. Defendants assumed a duty of care to use reasonable means to secure and safeguard this Personal Information, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of their data systems.

58. Defendants breached its duty of care by failing to secure and safeguard the Personal Information of Plaintiffs and other Class Members. Defendants negligently maintained

systems that they knew were vulnerable to a security breach, despite being made aware of these vulnerabilities any number of ways.

59. Defendants continue to breach this duty of care by failing to share crucial, complete information with Plaintiffs and other Class Members in a timely manner.

60. Plaintiffs and the other Class Members have suffered harm as a result of Defendants' negligence. These victims' loss of control over the compromised Personal Information subjects each of them to a greatly enhanced risk of identity theft, medical identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of fraud and theft. Plaintiffs and other Members of the proposed Class suffered and continue to suffer further harm by virtue of Defendants' failure to give timely and complete notice to them concerning the Breach and the risks they face.

61. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and every Member of the Class have been put at risk of identity theft and have an obligation to mitigate damages through credit monitoring services. Defendants are liable to each and every Member of the Class for the reasonable costs of future credit monitoring services. Defendants are also liable to those Class Members who have directly sustained damages as a result of their identity theft. Plaintiffs and Members of the Class have spent time and money to protect themselves as a result of Defendants' conduct, and will continue to be required to spend time and money protecting themselves, their identities, and their credit.

COUNT II - NEGLIGENCE *PER SE*

62. Plaintiffs repeat, re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

63. Pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"), Defendants had a duty to keep and protect the Personal Information of their customers and

provide notice to those affected without unreasonable delay and no later than 60 days after discovery of a breach. *See* 45 C.F.R. § 164.404.

64. Upon information and belief, Defendants violated HIPAA by failing to secure and safeguard Plaintiffs' and Class Members' Personal Information; by failing to implement protections against "reasonably anticipated threats" (45 C.F.R. § 164.306); and by failing to notify Plaintiffs and other Class Members in accordance with the requirements set forth in 45 C.F.R. §164.404.

65. Defendants' failure to comply with HIPAA, and/or other industry standards and regulations, constitutes negligence *per se*.

66. Plaintiffs and Members of the Class have been harmed as a result of Defendants' negligence *per se*. In the wake of the unauthorized release of their PHI and PII, Plaintiffs and Members of the Class have had to take steps– expending time and money -- to protect themselves against the greatly enhanced risk of identity theft, medical identity theft, credit and bank fraud, Social Security fraud, tax fraud and numerous other types of fraud and theft. Plaintiffs and Members of the Class have suffered and continue to suffer further harm as a result of Defendants' failure to give timely and complete notice to them concerning the Data Breach.

COUNT III - BREACH OF FIDUCIARY DUTY

67. Plaintiffs repeat, re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

68. Plaintiffs and Class Members, as customers of Defendants' business, have a special relationship with Defendants. Defendants owe a fiduciary duty to Plaintiffs and Class Members to keep their PHI and PII private and confidential and to protect it from misuse by others.

69. Defendants breached the fiduciary duty owed to Plaintiffs and Class Members by failing to adequately safeguard their PHI and PII against unauthorized disclosure and misuse.

70. Defendants further breached the fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify them of the breach of their PHI and PII.

71. Defendants' failure to adequately safeguard Plaintiffs' and Class Members' PHI and PII has resulted in losses and damages to Plaintiffs and Members of the Class.

72. Defendants continue to breach their fiduciary duties by failing to share crucial, complete information with Plaintiffs and other Class Members in a timely manner.

73. Plaintiffs and the other Class Members have suffered harm as a result of Defendants' breach of fiduciary duty. These victims' loss of control over the PII and PHI exposed subjects each of them to a greatly enhanced risk of identity theft, medical identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of fraud and theft. Plaintiffs and other Members of the proposed Class suffered and continue to suffer further harm by virtue of Defendants' failure to give timely and complete notice to them concerning the Breach and the risks they face.

74. Plaintiffs and other Class Members are entitled to injunctive relief as well as actual and punitive damages.

COUNT IV - BREACH OF CONTRACT OR, ALTERNATIVELY, IMPLIED CONTRACT

75. Plaintiffs repeat, re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein

76. When the Plaintiffs became insureds of Defendants, there arose a contract, either written or implied, between the Plaintiffs and Defendants. The same is true with respect to the contractual relationship that arose between Defendants and every other Member of the Class.

77. In exchange for compensation that was to be paid by Plaintiffs and by the Class, Defendants was to provide health insurance or health services.

78. Implicit in the agreement made by Defendants was an understanding that, as part of the health insurance or services to be provided to Plaintiffs and Members of the Class, Defendants would protect the sensitive information provided by Plaintiffs and the Class, as required by accepted law and the standards in Defendants' businesses.

79. Defendants breached their implied agreement causing damages to Plaintiffs and Members of the Class for which recovery should be made as demanded hereafter.

80. Defendants breached their contractual obligations by failing to secure and safeguard the PII and PHI of Plaintiffs and other Class Members. Defendants negligently maintained systems that they knew were vulnerable to a security breach, despite being made aware of these vulnerabilities any number of ways.

81. Defendants continue to breach their contractual obligations by failing to share crucial, complete information with Plaintiffs and other Class Members in a timely manner.

82. Plaintiffs and the other Class Members have suffered harm as a result of Defendants' breach of contract. These victims' loss of control over the Personal Information exposed subjects each of them to a greatly enhanced risk of identity theft, medical identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of fraud and theft. Plaintiffs and other Members of the proposed Class suffered and continue to suffer further harm by virtue of Defendants' failure to give timely and complete notice to them concerning the Breach and the risks they face.

83. Plaintiffs and Class Members seek actual damages as described herein to be proven at trial, as well as attorneys' fees and costs as permitted by law.

COUNT V - VIOLATION OF THE NEW YORK DECEPTIVE ACTS AND PRACTICES LAW
(N.Y. GEN. BUS. § 349, *et seq.*)

84. Plaintiffs repeat, re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein

85. New York General Business Law § 349 ("GBL 349") makes unlawful deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of a service in this state.

86. Plaintiffs are consumers as defined by GBL 349.

87. Defendants' providing of health care services as described herein constitutes the conduct of any trade or commerce or furnishing services in this state within the meaning of GBL

88. In the conduct of their business, trade and commerce, and in their furnishing services in this state, Defendants' actions were directed at consumers.

89. In the conduct of their business, trade and commerce, and in their furnishing services in this state, Defendants collected and stored Personal Information belonging to Plaintiffs and Class Members.

90. In the course of Defendants' business of selling insurance coverage and providing medical services to consumers, they willfully failed to disclose that their cybersecurity systems were inadequately protected and that their cybersecurity policies and procedures were inadequately implemented. In turn, Defendants willfully made affirmative representations that customers' PII and PHI would be safe. Furthermore, Defendants willfully failed to disclose the Breach to Plaintiffs and Class Members for more than four weeks.

91. Accordingly, Defendants made untrue, deceptive, and misleading representations of material facts and omitted and/or concealed material facts to Plaintiffs and the Class.

92. In reality, Defendants failed to provide adequate protection to their customers' Personal Information, resulting in the Breach.

93. The security of Defendants' data systems was a material fact to Plaintiffs and the Class. Had Plaintiffs and the Class known of Defendants' misrepresentations and omissions as described herein, they would not have purchased health coverage or medical services from Defendants or provided their Personal Information to Defendants.

94. Plaintiffs and the Class suffered injury caused by Defendants' affirmative statements, as well as their failure to disclose material information.

95. Plaintiffs and the Class overpaid for their medical coverage and did not receive the benefit of their bargain, as a portion Defendants' premiums were purported to provide cybersecurity to their PHI and PII.

96. Pursuant to GBL 349, Plaintiffs and the Class are entitled to recover the greater of actual damages or $50. Because Defendants acted willfully or knowingly as described herein, Plaintiffs and the Class are entitled to recover three times their actual damages, up to $1,000.

COUNT VI - BAILMENT

97. Plaintiffs repeat, re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

98. Plaintiffs and the Class delivered and entrusted their PHI and PII to Defendants for the sole purpose of obtaining health insurance and/or medical treatment.

99. During the time of bailment, Defendants owed Plaintiffs and the Class Members a duty to safeguard this information properly and maintain reasonable security procedures and practices to protect such information.

100. Defendants breached their bailment and their duty of care by failing to take appropriate measures to safeguard and protect the PHI and PII of Plaintiffs and the Class. This breach resulted in the unlawful and unauthorized access to and misuse of the PII and PHI of Plaintiffs and the Class.

101. Defendants further breached their bailment and their duty to safeguard the Personal Information of Plaintiffs and the Class by failing to timely and completely notify Plaintiffs and the Class that their PII and PHI were compromised as a result of the Breach.

102. As a result of Defendants' Breach, Plaintiffs and the Class have suffered monetary damages and will continue to be injured and incur damages in the future both in an effort to protect themselves and to remedy acts of fraudulent activity. Plaintiffs and the Class have suffered and/or are reasonably likely to suffer theft of PHI and PII; costs associated with prevention, detection, and mitigation of identity theft and/or fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of fraud in any of their myriad forms; and damages from the unconsented exposure of personal and health information due to this breach.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct

complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and Class Members;

C. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

D. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined;

E. For an award of punitive damages;

F. For an award of costs of suit and attorneys' fees, as allowable by law; and

G. Such other and further relief as this court may deem just and proper.

JURY DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

Dated: November 6, 2015

By: /s/ James J Bilsborrow

WEITZ & LUXENBERG, P.C.
James J Bilsborrow (NY Bar No. 4702064)
700 Broadway
New York, NY 10003
(212) 558-5500
Email: jbilsborrow@weitzlux.com

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
John A. Yanchunis*
Florida Bar No. 324681
201 North Franklin Street 7th Floor
Tampa, Florida 33602
(813) 223-5505
Email: jyanchunis@forthepeople.com

LAW OFFICE OF JEAN SUTTON MARTIN PLLC
Jean Sutton Martin*

North Carolina Bar No. 25703
2018 Eastwood Road, Suite 225
Wilmington, North Carolina 28403
(910) 292-6676
Email: jean@jsmlawoffice.com

LAW OFFICE OF PAUL C. WHALEN, P.C.
Paul C. Whalen (PW1300)
768 Plandome Road
Manhasset, NY 11030
(516) 426-6870
Email: pcwhalen@gmail.com

Attorneys for Plaintiffs and the Proposed Class

** Pro Hac Vice application to be submitted*